Défis posés par l'identification par utilisateur et l'application des politiques dans la passerelle Web sécurisée (SWG) pour les environnements d'ordinateurs partagés avec authentification SAML et transfert de trafic basé sur PAC

Table des matières

Problème

Dans les déploiements Cisco Secure Web Gateway (SWG) utilisant l'accès sécurisé avec authentification SAML et le transfert de trafic PAC ou Branch vers Internet, seul le premier utilisateur connecté à un ordinateur partagé est correctement identifié pour le trafic Web et l'application de la stratégie. Lors de la commutation d'utilisateurs, le trafic Web suivant continue d'être attribué à l'utilisateur initial, même lorsque l'option de substitution IP est désactivée et qu'un fichier PAC est utilisé. Les requêtes DNS reflètent l'utilisateur actif correct via Umbrella Virtual Appliance, mais les journaux Web et de pare-feu mappent constamment l'activité à l'utilisateur précédent. La demande consiste à déterminer si SWG prend en charge l'identification par utilisateur et l'application de la stratégie dans les environnements d'ordinateur partagé et comment assurer un mappage utilisateur correct.

Environnement

- Appareil virtuel pour la résolution DNS.
- Authentification SAML pour l'identité utilisateur.
- Combinaison de transfert de trafic avec PAC et sans fichiers PAC.
- Option de substitution IP activée, avec des sous-réseaux et des hôtes spécifiques contournés pour la substitution de cookie.
- Périphériques sur site ; pas de terminaux ou d'utilisateurs distants.

Résolution

Le problème a été résolu par la formation des utilisateurs et les conseils de configuration en gardant à l'esprit les points suivants :

- Utiliser l'identification de substitution de cookie avec les fichiers PAC. Le trafic peut être acheminé vers ou depuis un tunnel réseau.
- Utilisez l'identification de substitution de cookie sans fichiers PAC, mais le trafic doit passer

par un tunnel réseau.
- L'authentification SAML doit être activée dans le profil de sécurité de la stratégie d'accès que vous souhaitez appliquer la substitution de cookie.
- Le trafic de substitution de cookie est réservé au trafic basé sur navigateur. Une règle distincte est nécessaire pour identifier le trafic non-cookie de l'ordinateur (par exemple, le trafic Teams ou Webex) avec l'identité source comme réseau.
- Le module SWG ne doit pas être utilisé pour que le substitut de cookie fonctionne.
- Lorsque la substitution IP est également activée, vous devez ajouter les adresses IP/sous-réseaux privés qui ont l'intention d'utiliser la substitution de cookie dans la liste de contournement (Utilisateurs et groupes - Gestion de la configuration - Paramètres avancés).
- La liste de contournement du substitut de cookie correspond également à des préfixes plus courts. Par exemple, si vous ajoutez 10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- Le substitut de cookie prend en charge la commutation d'un utilisateur à partir d'une machine sans avoir à se déconnecter pour conserver plusieurs identités.

Une grande partie du dépannage a été le test des stratégies et la recherche d'activité.

Motif

La cause principale de l'identification incorrecte des utilisateurs dans les environnements d'ordinateurs partagés est principalement due à l'éducation des utilisateurs.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.